

64934 U.S. PAT. & TM. OFF. 05/22/97

COMMISSIONER OF PATENTS  
AND TRADEMARKS  
Washington, D.C. 20231

Sir:

Transmitted herewith for filing  
is the patent application of

inventor(s): Dillard, et al.

For: COPY PROTECTION FOR DATABASE  
UPDATES TRANSMITTED VIA THE  
INTERNET

Enclosed are:

- (x) 9 sheet(s) of drawing ( ) Informal  
(X) Assignment of the invention to ALLIEDSIGNAL, INC.  
( ) The assignment fee of \$40 to cover the recording of the assignment is  
to be charged to Deposit Account No. 06-1135.  
(x) Executed Declaration  
(X) Information Disclosure Statement, Form PTO-1449 with references.

Fee Calculation For Claims As Filed

|                                      |   |                  |
|--------------------------------------|---|------------------|
| a) Basic Fee                         |   | \$ 770.00        |
| b) Independent Claims                | <u>2</u> - <u>3</u> = <u>0</u> x \$ 80.00 =   | \$ <u>0</u>      |
| c) Total Claims                      | <u>18</u> - <u>20</u> = <u>0</u> x \$ 22.00 = | \$ <u>0</u>      |
| d) Fee for Multiply Dependent Claims | \$260.00                                      | \$ <u>0</u>      |
| Total Filing Fee                     |   | \$ <u>770.00</u> |

- ( ) Statement(s) of Status as Small Entity,  
reducing Filing Fee by half to \$ 0
- (x) A check in the amount of \$ 810.00 to cover the filing fee.
- ( ) Charge \$ 0 to Deposit Account No. 06-1135.
- ( ) The payment of the Filing Fee is to be deferred until the Declaration  
is filed. Do not charge our Deposit Account.
- (X) The Commissioner is hereby authorized to charge any additional fees  
which may be required in this application under 37 C.F.R. §§1.16-  
1.17 during its entire pendency, or credit any overpayment, to Deposit  
Account No. 06-1135. Should no proper payment be enclosed herewith,  
as by a check being in the wrong amount, unsigned, post-dated,  
otherwise improper or informal or even entirely missing, the  
Commissioner is authorized to charge the unpaid amount to Deposit  
Account No. 06-1135. This sheet is filed in triplicate.

135 S. LaSalle Street-Suite 900  
Chicago, Illinois 60603-4277  
(312) 372-7842

FITCH, EVEN, TABIN & FLANNERY

By: John S. Paniaguas  
John S. Paniaguas  
Registration No. 31,051

PATENT APPLICATION

Attorney Docket No. 60323  
Date: May 22, 1997

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"Express Mail" Mailing Label Number

EH 607069675US

Date of Deposit May 22, 1997

I hereby certify that this paper or fee is being  
deposited with the United States Postal Service  
"Express Mail Post Office to Addressee" Service  
under 37 CFR §1.10 on the date indicated above  
and is addressed to the Commissioner of Patents  
and Trademarks, Washington, D.C. 20231.

ED PRICE

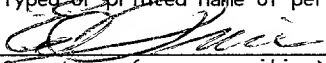
(Typed or printed name of person mailing)

(Signature of person mailing)

Attorney Docket 60323/462-96-004  
CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"Express Mail Mailing Label Number  
EH607069675US

Date of Deposit May 22, 1997  
I hereby certify that this paper or fee is  
being deposited with the United States Postal  
Service "Express Mail Post Office to  
Addressee" Service under 37 CFR §1.10 on the  
date indicated above and is addressed to the  
Assistant Commissioner for Patents,  
Washington, D.C. 20231.

ED PRICE  
(Typed or printed name of person mailing)  
  
(Signature of person mailing)

## **COPY PROTECTION FOR DATABASE UPDATES TRANSMITTED VIA THE INTERNET**

### **CROSS REFERENCE TO RELATED APPLICATIONS**

5

The present application is based upon and  
claims priority of U.S. Provisional Application No.  
60/021,702, filed on July 12, 1996.

10

### **BACKGROUND OF THE INVENTION**

#### **1. Field of the Invention**

15 The present invention relates to a system for  
protecting the unauthorized use of software transmitted  
over a communication link and more particularly to a  
system in which the software is encrypted with a unique  
software key that only allows the software to be  
uploaded into a unit, such as global positioning system  
(GPS) unit, with a matching software key.

#### **2. Description of the Prior Art**

20

Global positioning systems are known to be used  
in aircraft and other vehicles for navigation. Such GPS  
systems not only provide the position of the aircraft or  
vehicle but may also be integrated with topographical  
and/or navigational data, such as terrain and airport  
25 topographical data as well as highway maps stored in a

database, to provide an indication of the vehicle or aircraft relative to the topographical data or highway information. For example, as disclosed in U.S. Patent Application Serial No. 08/509,642 filed on July 31,  
5 1995, assigned to the same assignee of the present invention, the topographical data, such as the elevation of the highest obstacles within a predetermined region, are stored in a memory device aboard the aircraft. The GPS allows the topographical data to be displayed as a  
10 function of the position of the aircraft.

Often times, the topographical and navigational data needs to be updated due to changing topography and highway information. Because of the relative ease in which software that is transmitted over the Internet can  
15 be duplicated, updates of the topographical data is known to be provided in a diskette or cartridge form and mailed to the customers. Typically, users of such integrated GPS systems must first determine if an update is available by checking with the database vendor.  
20 Orders are typically placed by telephone. The update diskette or cartridge is then mailed to the customer. As such, from the time the order is placed, considerable time passes before the updated topographical data is actually received by the customer so it can be uploaded  
25 into the customer's integrated GPS unit. The delay is even more acute for international customers for which the mailing time is considerably greater.

There are other problems associated with providing updated topographical and navigational data on  
30 diskettes or cartridges to a customer. For example, for customers that have multiple integrated GPS units, the customer may choose to upload the updated data onto such multiple units even though the customer has only paid for the update for a single unit. The customer may also  
35 transfer the update diskette or cartridge to another unauthorized user.

### **SUMMARY OF THE INVENTION**

It is an object of the present invention to solve various problems in the prior art.

It is yet another object of the present  
5 invention to provide a system for preventing unauthorized use of a database or other software transmitted over a communication link, such as the Internet.

Briefly, the present invention relates to a  
10 system for transmitting a database or other software over a communication link, such as the Internet, which prevents unauthorized use. In order to prevent such unauthorized use, the customer's equipment, such as a GPS unit, is provided with a unique software key. The  
15 updated database is ordered over the communication link by providing the unique software key and may include electronic payment information. The database is encrypted, for example, as a function of the unique software key and transmitted over the communication link  
20 in encrypted form along with an upload program. The upload program only allows the encrypted database to be uploaded into a unit with a matching software key. As such, the system allows updated databases to be transmitted rather quickly and easily over a  
25 communication link while preventing unauthorized use.

### **DESCRIPTION OF THE DRAWINGS**

These and other objects of the present  
invention will be readily understood with reference to  
30 the following specification and attached drawings wherein:

FIG. 1 is a graphical illustration of an exemplary Internet page layout in accordance with the present invention;

35 FIG. 2 is a simplified representation of a dialog box which may form a part of one of the Web pages

for user information, such as the unique software key,  
in accordance with the present invention;

FIG. 3 is a simplified view of a personal  
computer interfacing with an Internet server in order to  
5 provide user information;

FIG. 4 is similar to FIG. 2 illustrating the  
process of downloading the software from the Internet to  
a user's personal computer;

FIG. 5 is a simplified graphical representation  
10 illustrating the uploading of the software from the  
Internet being transferred between a personal computer  
and a product, such as an integrated global positioning  
system (GPS) unit;

FIG. 6 is a block diagram illustrating the data  
15 flow and the organization of the software on the  
Internet server in accordance with the present  
invention;

FIG. 7 is a simplified flowchart illustrating a  
portion of the system in accordance with the present  
20 invention for ordering software over the Internet;

FIG. 8 is a graphical representation of a  
dialog box for user payment information which may form a  
portion of one of the Web pages illustrated in FIG. 1 in  
accordance with the present invention;

FIG. 9 is a graphical illustration of a dialog  
25 box for enabling users to provide information regarding  
the requested software as well as a unique software key  
which may form a portion of one of the Web pages  
illustrated in FIG. 1 in accordance with the present  
30 invention;

FIG. 10 is a graphical illustration of a dialog  
box for the user's desired payment method which may form  
a portion of one of the Web pages illustrated in FIG. 1  
in accordance with the present invention;

FIG. 11 is a graphical illustration of a  
35 confirmation page which may form a portion of one of the

2025 RELEASE UNDER E.O. 14176

Web pages illustrated in FIG. 1 which enables the user to download software over the Internet in accordance with the present invention;

FIG. 12 is a flowchart of the system in accordance with the present invention which provides copy protection for software transferred over the Internet in accordance with the present invention;

FIG. 13 is a flowchart of the software at the server for encrypting the software to be transferred over the Internet in accordance with the present invention; and

FIG. 14 is a flowchart of the decryption process for uploading software transferred over the Internet to a customer's unit, such as an integrated global positioning system (GPS) unit.

#### **DETAILED DESCRIPTION**

The present invention relates to a system for preventing unauthorized use of a database or other software transmitted over a communication link, such as the Internet, for use in particular electronic equipment, such as a global position system (GPS) unit. As mentioned above, such systems utilize topographical data for various regions of the world in order to display the topographical data as a function of the position of the aircraft. Heretofore such GPS units have been sold with topographical and/or navigational data stored in a database on cartridges or diskettes. Updated databases are known to be shipped through the mail. Such a process takes a relatively long period of time. The system in accordance with the present invention allows the database update to be transmitted over communication links, such as the Internet quickly and easily while virtually eliminating unauthorized use of the database information. More particularly, each GPS unit is provided with a unique software key. The

unique key is an 8 digit hexadecimal number, which may be embedded in a read only memory (ROM) within the GPS unit or stored within a removable cartridge at the factory prior to a GPS unit being shipped to the customer. The user uses the unique software key to order update software, such as an update database for the GPS unit, over the communication link and upload the database into a GPS unit with a matching software key, for example as illustrated in FIGS. 3, 4 and 5. For example, the user simply connects to the GPS database or other software vendor's home page on the WorldWide Web. After providing the unique software key number as well as the desired payment method, the database or other software is encrypted as a function of the unique software key at the Internet server, for example. The encrypted software is transmitted to the user over the Internet along with a decryption program which only allows the software to be uploaded into a GPS unit having a matching key. Since the updated database is encrypted as a function of the unique software key, any attempts to upload the software into a unit not matching the unique software key will be futile. Although multiple copies of the encrypted database can be made, the system in accordance with the present invention prevents these encrypted copies from being uploaded into multiple GPS units.

The present invention is suitable for updating the topographical information stored in databases for use with various integrated GPS systems, such as, KLX 100 GPS/COMM, KLN 98/KLN 89B GPS, KLN 90B GPS and KLN 900 GPS, available from AlliedSignal, Incorporated. Although the system in accordance with the present invention is described and illustrated in terms of transferring updated database information for an integrated GPS over the Internet, the principles of the present invention are clearly applicable to protecting

virtually any type of software transmitted over  
virtually any communication link; wired or wireless.

It is also to be understood that the principles  
of the present invention are also applicable to other  
5 forms of electronic transfer that do not involve the  
Internet and may be implemented for transferring  
software over virtually any communication link, such as  
a modem and even a wireless link. Moreover, as will be  
discussed in more detail below, a personal computer is  
10 used to access the Internet server, for example, which  
contains the software to be transferred as illustrated  
in FIGS. 3 and 4. The desired software is then  
encrypted and transferred along with a decryption  
program back to the personal computer, which, in turn,  
15 is used to transfer and decrypt the software into a  
separate electronic unit, such as an integrated GPS  
unit. However, it should also be understood that the  
principles of the present invention are also applicable  
to systems in which the desired software is also  
20 transmitted from a remote communication node, such as an  
Internet server, directly to the unit, such as the  
integrated GPS unit itself.

Referring to FIG. 1, an exemplary Web page  
layout is illustrated. The exemplary Web page layout  
25 includes a home page 22. The home page 22 is provided  
with one or more hyperlinks to provide access to the  
succeeding Web pages. As shown, the home page 22, for  
example, as illustrated in FIG. 8, may be provided with  
a hyperlink to a database selection page 24 (FIG. 9).  
30 The database selection page 24 enables a user to select  
the specific database. As mentioned above, depending  
upon the type of integrated GPS unit, various update  
databases are available for transfer over the Internet.  
After the particular database is selected from the  
35 database selection page 24, a hyperlink may be provided  
to a method of payment Web page 26 with hyperlinks to a



credit card Web page 28 (FIG. 10) and a user password Web page 30. It is to be understood that the payment option is merely optional. The credit card Web page 28 and the user password Web page 30 allow alternate  
5 payment methods for the user in systems which include electronic payment. The credit card Web page 28 requires the user's credit card information as well as the unique software key (FIG. 2). Alternatively, the system allows for the customer to contact the software  
10 supplier ahead of time and establish an account. In this situation the user merely enters a password for the account as well as the unique software key for the unit. The credit card Web page 28 and the password Web page 30 are provided with hyperlinks to a confirmation page 32  
15 (FIG. 11). The confirmation page 32 is merely exemplary and is not required for practice of the invention. The confirmation page 32 confirms the user's selection for the particular database as well as the method of electronic payment. If the user enters a confirmation,  
20 a hyperlink may be provided on the confirmation page 32 to initiate downloading of the updated software, which is linked to a message page 34 which indicates downloading in progress.

FIGS. 3 through 7 illustrate the present  
25 invention. As shown, user information is transferred over the Internet to one or more Internet servers 36 by way of a personal computer which may be an IBM compatible personal computer or other personal computer  
suitable for connection to the Internet. The software  
30 is encrypted and then transferred from one or more Internet servers 36 back to the personal computer 38 along with a decryption and upload program. The upload program enables the encrypted database to be uploaded into a product with a matching software key, such as an  
35 integrated GPS unit 40.

The software layout for the system is illustrated in FIG. 6 and includes a user database 40, a master "nav" database 42 and an upload program 44, identified as NETLOAD.EXE. The user information for example, regarding account and password information, etc. is maintained in the user database 40, accessible by the server 36. The topographical information is stored in the master "nav" database file 42, also accessible by the server 36. Once the user provides the unique software key as well as the desired payment method, a copy of the topographical and/or navigation data from a master "nav" file 42 is encrypted as a function of the unique software key, provided by the user and stored in a "keyed DB file" 44. The keyed DB file 44 is then compressed into a zip file 46 and transferred to the user by way of the Internet along with the decryption or upload file 44, identified as NETLOAD.EXE. The decryption file 44 enables the zip file containing the encrypted database to be uploaded into a product 40 as long as the software key of the product matches the software key to which the database was encrypted. If the software key matches the unique key within the product, the database is decrypted and uploaded into the product.

A simplified flowchart for the system in accordance with the present invention is illustrated in FIG. 7. Initially, the user connects to the database vendor's home page in step 48. Once connected to the database vendor's home page, the user selects a database from the available databases in step 50. Steps 52 and 54 provide for alternate payment methods. If a user wishes to avoid providing credit information over the Internet, the user can obtain a password and an account and become a registered user. Thus, the system checks whether the user is a registered user in step 52. If not, the system assumes the payment will be made by

credit card in step 54. In both steps 52 and 54, the user also provides the unique software number that is used to encrypt the database as a function thereof. After the payment method and unique software key are entered, a confirmation page is generated in step 56, for downloading the software.

An overall flow chart is illustrated in FIG. 12. Initially, the unique software key, for example, the 8 digit unique software key unique to the GPS system, is read from the GPS unit 40 by the user and entered on the appropriate Web pages as discussed above. The software key may be printed somewhere on the GPS unit 40 to enable the user simply visually read the software key from the unit in step 58. In step 60, the user logs onto the Internet, chooses a database product and provides the unique software key for the GPS unit 40. The system encrypts the selected database as a function of the unique software key and stored into a keyed database file 44 (FIG. 6) in step 62. In order to conserve storage space, the keyed database file 44 may also be compressed in step 63 and transferred to the customer personal computer 38 in step 64 along with a decryption program 44, identified as NETLOAD.EXE. The keyed database file is then uploaded by the user to their GPS unit 40 (FIG. 5) with a matching software key in step 66.

The flowchart for the database encryption or keying is illustrated in FIG. 13. After the user logs onto the Internet, selects a database and provides the unique software key, the system checks in step 68 whether the desired database is a type KLN 90 database. As used herein the KLN 90 type databases relates to the type of processor within the GPS unit 40. In particular, KLN 90 type databases are formatted for use with Intel type processor chips, while the balance of the databases are formatted for use with Motorola type

processor chips. Due to the different byte storage methods between the two processor styles, the system checks in step 68 whether request is for a type KLN 90 database. If so, a temporary file is created in step 70 with the database key embedded into the original KLN 90 file from a master KLN 90 database file 72, a subset of the master "nav" DB files 42. If the request is for other than KLN 90 type database, the system proceeds directly to step 74. In step 74, starting with the first byte, the byte is encrypted as a function of the database key, for example by cyclic redundancy coding (CRC), as discussed below. After the first byte is coded with the database key, the key is updated for the next byte in step 76. The keyed or encrypted byte is written to an output file 82 for later transmission over the Internet to the user's personal computer 38 in step 78. This process is continued until all of the bytes in the database file have been keyed and written to the output file 82 as illustrated by step 80. After all of the bytes have been written to the output file 82, a footer tag with data from the original file, including checksums, file size, database type, the effective dates and the original database key are written to the output file 82 and sent to the user along with the upload file NETLOAD.EXE in step 82 as discussed above. If the software key in the GPS unit 40 matches the database key, the NETLOAD.EXE file decrypts and uploads the updated database into an integrated GPS unit 40.

FIG. 14 is a flowchart for the decryption program 44 (NETLOAD.EXE) for uploading the encrypted database software to the GPS unit 40. As mentioned above, the encrypted database file 82 is provided with the encrypted data as well as a footer tag which includes the original software key, checksums, the file size, the database type as well as the effective dates for the database. In step 86, the footer tag is read



full, a packet of decrypted data is sent to the GPS unit 40 in step 114. As indicated in step 116, the process is repeated until all of the bytes in the encrypted database file have been processed.

5           Essentially the encryption process is based on cyclic redundancy code (CRC) table of 256 pseudo random numbers from 0 to 255, for example, as illustrated in TABLE 1.

TABLE 1

|    |                 |            |
|----|-----------------|------------|
| 10 | CRC TABLE ENTRY | VALUE      |
|    | 0               | 0          |
|    | 1               | 1996959894 |
|    | 2               | 3993919788 |
|    | 3               | 2567524794 |
| 15 | ...             |            |
|    | 114             | 3188396048 |
|    | ...             |            |
|    | ...             |            |
|    | 141             | 2466906013 |
| 20 | ...             |            |
|    | ...             |            |
|    | 237             | 3736837829 |
|    | ...             |            |
| 25 | 255             |            |

Initially, a seed CRC value is chosen, for example 13579246. The first byte in the database or source file is read and added to the seed value. For example, if the first byte in the database equates to the number 3, the new byte will be the CRC seed value (13579246) plus the byte read from the file Boolean ANDed with the hexadecimal number FF or 255. For example, adding the value of the source byte 3 to the seed value of 13579246 would equal the number 13579249.



The process is repeated for each byte in the file, for example as shown in TABLE 4 below.

TABLE 4

| BYTE NUMBER | ORIGINAL DATA FILE | NEW DATA FILE | CRC KEY (START = 13579246) |
|-------------|--------------------|---------------|----------------------------|
| 1           | 3                  | 241           | 3736818166                 |
| 2           | 132                | 122           | 3201674049                 |
| 3           | 204                | 13            | 2478254646                 |

The process is repeated for each byte in the file.

In order to decode or decrypt the data bytes, the process is simply reversed starting with the same known seed CRC key and the same base CRC table values, for example as illustrated in TABLE 5 below.

TABLE 5

| BYTE NUMBER | KEY DATA FILE | NEW DATA FILE | CRC KEY (START = 13579246) |
|-------------|---------------|---------------|----------------------------|
| 1           | 241           |               |                            |
| 2           | 122           |               |                            |
| 3           | 13            |               |                            |

Initially, the first byte from the keyed file is read, for example 241. The current value of the CRC key (13579246) is subtracted from that value. The result (-13579005) is Boolean ANDed with 255 which provides a result of 3 which was the original starting point for example as shown in TABLE 6 below.

TABLE 6

| BYTE NUMBER | KEY DATA FILE | NEW DATA FILE | CRC KEY (START = 1359246) |
|-------------|---------------|---------------|---------------------------|
| 1           | 241           | 3             |                           |
| 2           | 122           |               |                           |



| BYTE NUMBER | KEY DATA<br>FILE | NEW DATA<br>FILE | CRC KEY<br>(START =<br>1359246) |
|-------------|------------------|------------------|---------------------------------|
| 3           | 13               |                  |                                 |

The CRC key is then updated for the next byte. In order to update the CRC key essentially the same method is used as before. The new byte 3 is EXCLUSIVE ORed with the current value of the CRC key (13579246). The result (13579245) is then Boolean ANDed with the hexadecimal number 255 with a result of 237 which is used as an index to look the CRC value in the CRC lookup table. The current example of the index corresponds to a table value of 3736837829. The current CRC key (13579246) is then shifted to the right 8 places. The result 53043 is EXCLUSIVE ORed with the value that was looked up in the CRC table (3736837829) by way of the index 237. The result 3736818166 is the CRC for the new byte, for example as shown in TABLE 7 below.

TABLE 7

| BYTE NUMBER | KEY DATA<br>FILE | NEW DATA<br>FILE | CRC KEY<br>(START =<br>13579246) |
|-------------|------------------|------------------|----------------------------------|
| 1           | 241              | 3                | 3736818166                       |
| 2           | 122              |                  |                                  |
| 3           | 13               |                  |                                  |

For the next byte the current CRC key 3736818166 is subtracted from the next byte read 122, the result being 558149252. This result 558149252 is anded with the hexadecimal number 255 to produce the next byte 132 which, is the original byte number in the original data file. The process is repeated for each byte as shown below in TABLE 8.

TABLE 8

| BYTE NUMBER | KEY DATA<br>FILE | NEW DATA<br>FILE | CRC KEY<br>(START =<br>13579246) |
|-------------|------------------|------------------|----------------------------------|
| 1           | 241              | 3                | 3736818166                       |
| 2           | 122              | 132              | 3201674049                       |
| 3           | 13               | 204              | 2478254646                       |

The process is repeated until the end of the file and the end result is that the output file exactly corresponds to the original file which was encrypted.

Obviously, many modifications and variations of the present invention are possible in light of the above teachings. Thus, it is to be understood that, within the scope of the appended claims, the invention may be practiced otherwise than as specifically described above.

What is claimed and desired to be secured by Letters Patent of the United States is:

**WE CLAIM:**

1. A method for preventing unauthorized use of software transmitted over a communication link, the  
5 method comprising the steps:

(a) providing an electronic unit with a unique software key;

(b) encrypting the software to be transmitted as a function of said unique software key; and

10 (c) transmitting the encrypted software over said communication link.

(d) providing an upload program which only allows for uploading of said software into an electronic unit with a matching software key.

15

2. The method as recited in Claim 1, wherein said software key is embedded in the electronic unit in which the requested software is to be uploaded.

20

3. The method as recited in Claim 1, wherein said electronic unit is a global positioning system (GPS) unit.

25

4. The method as recited in Claim 3, wherein said unique software key is embedded in said GPS unit.

5. The method as recited in Claim 1, wherein said encrypting step includes cyclic redundancy coding (CRS).

30

6. The method as recited in Claim 5, where said unique software key is initially used as a seed for encrypting said software.

35

7. The method as recited in Claim 1, wherein said communication link is wired link.



16. The system as recited in Claim 13, wherein said encrypting means utilizes cyclic redundancy coding for encrypting said software.

5           17. The system as recited in Claim 16, wherein said unique software key is initially used as a seed for encrypting said software.

10           18. The system as recited in Claim 13, wherein said communication link is a wired link.

15           19. The system as recited in Claim 13, wherein said uploading means includes means for decrypting said encrypted software.

          20. The system as recited in Claim 14, wherein said software is topographical data.

44380" 606T9880



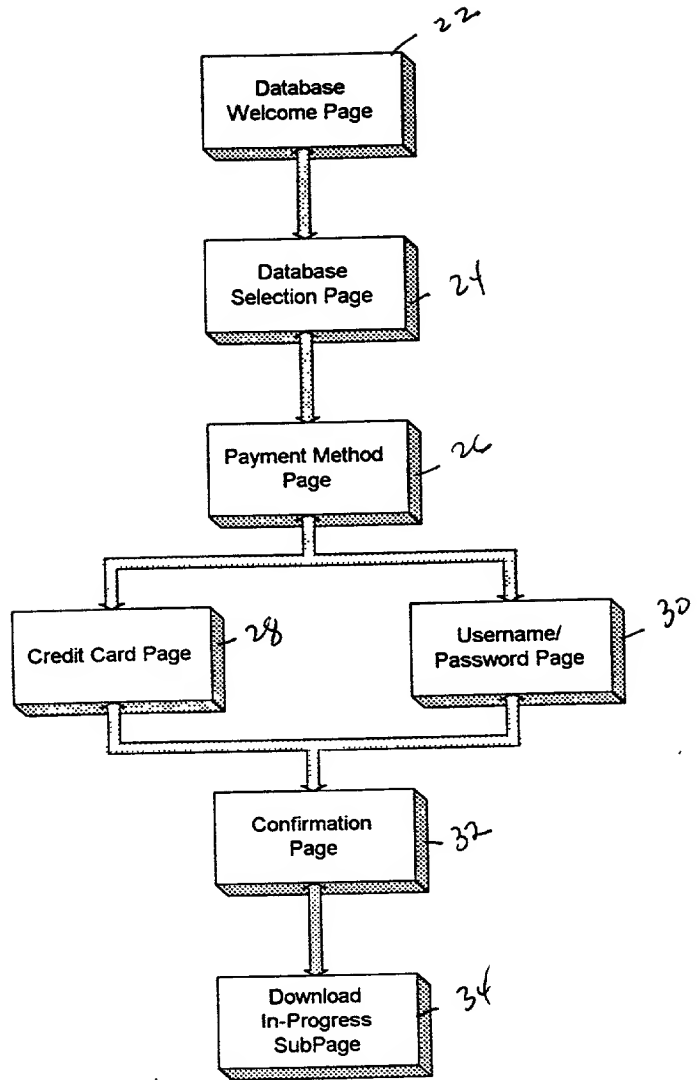


FIG 1

08861989.052297

|                                 |   |
|---------------------------------|---|
| 32.5 nm<br>KIXD<br>Leg<br>SET 3 | Update DB on<br>ground only<br>Key 1782A949<br>Update pub DB? |
|---------------------------------|---|

**← Database Key needed for download**

FIG 2.

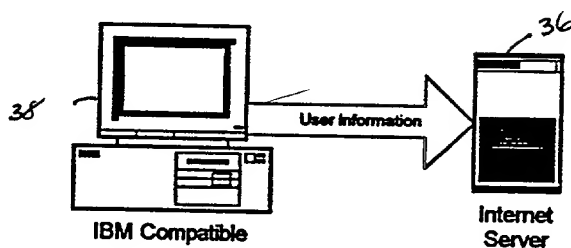


FIG 3

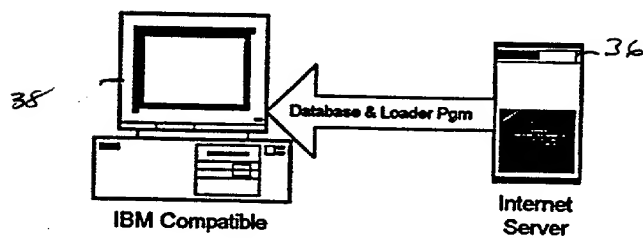


FIG. 4



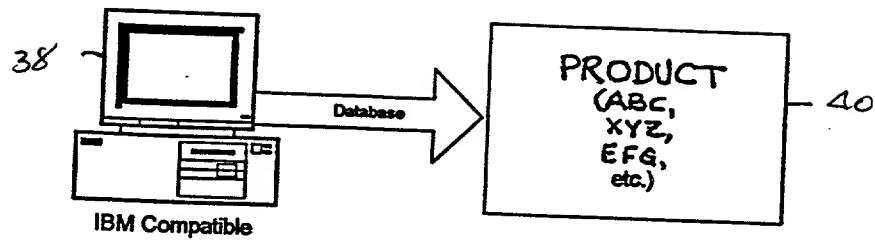


FIG. 5

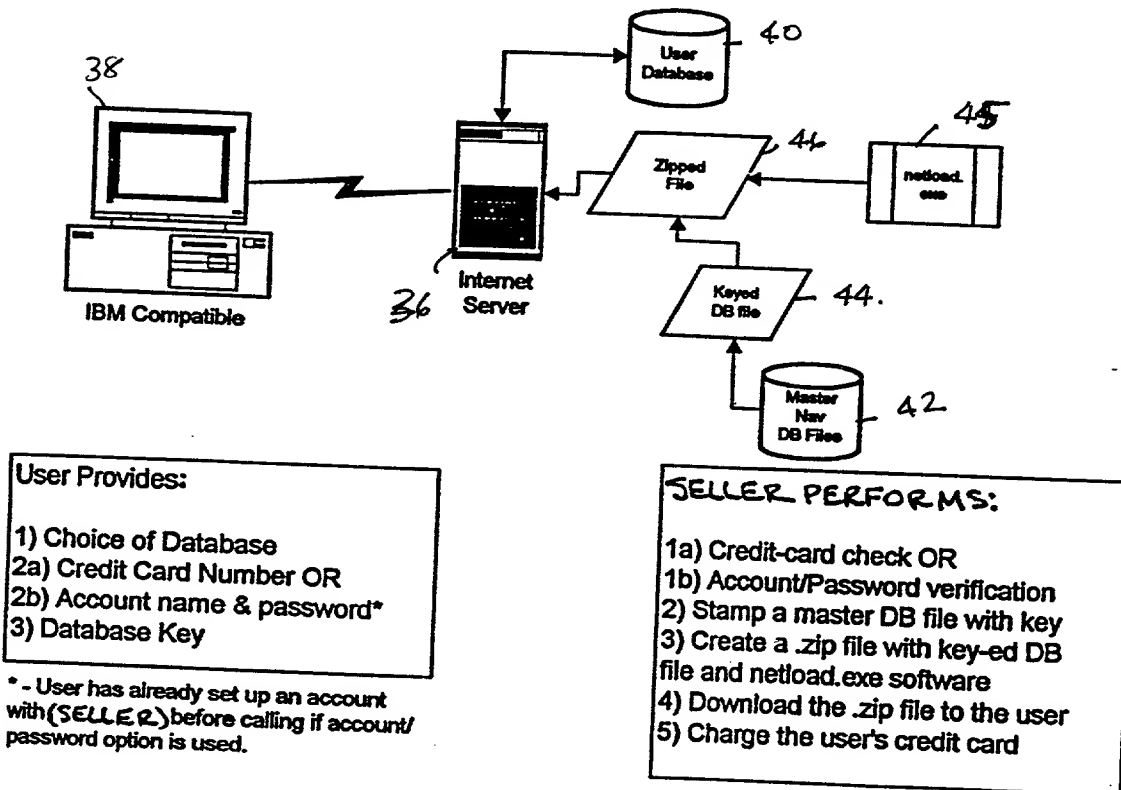


FIG 6.

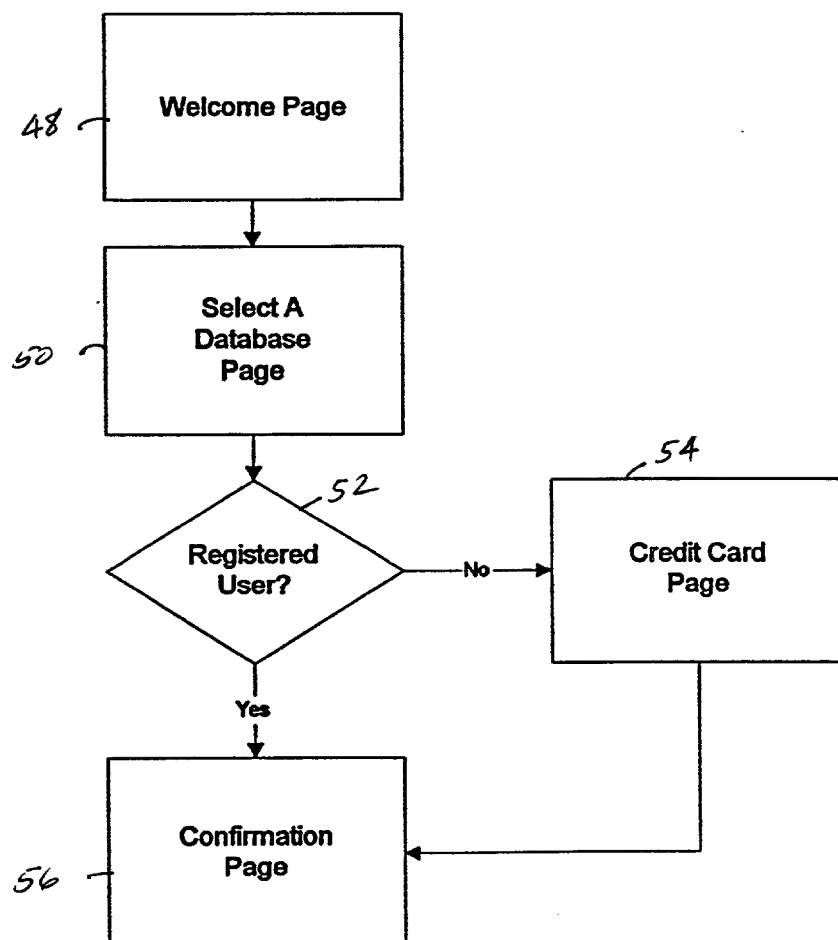


FIG. 7

Welcome to the (Seller) Database Update Center

If you have a pre-existing account set up with us, enter your name and password here:

NAME : \_\_\_\_\_

PASSWORD: \_\_\_\_\_

SUBMIT Name & Password

OR

Select a Database, and we will ask you for a credit-card later.

Select a Database // FAQ // Back to (Seller) Home Page // What do I need for this? // Feedback

22

FIG. 8

24  
Select a Database

If you would like to see a price list, Press Here.

If you would like information on database coverage areas, Press Here.

Want to know how big the files are before you download? Press Here.

What type of product is this database for? \_\_\_\_\_ (Drop-down Choice Box)

What is the 8-char Database Key for the unit? \_\_\_\_\_ Example: 0012A4C5 Help

SUBMIT

FAQ // Back to (Seller) Home Page // What do I need for this? // Feedback

FIG. 9

FIG 11



```

graph TD
    A[Database requested  
8-hex digit DB Key  
unique to hardware] --> B{Is this for a KLN90-  
style database?}
    B -- No --> C[Starting at byte 1, code  
the byte in the master  
file with the key]
    B -- Yes --> D[Create a temporary file  
with DB Key imbedded  
into original KLN90 file]
    E[Other Master DB files] --> C
    F[Master KLN90 files] --> D
    D --> C
    C --> G[Update the key for the  
next byte]
    G --> H[Write the key-ed byte  
to output file]
    H --> I[Repeat for each byte in  
master file]
    I --> C
    I --> J[Write footer tag with  
data from original file,  
including checksums,  
file size, database  
type, effective dates,  
and original DB Key]
    J --> K[/New file with  
key-ed data  
and footer tag  
database.dat/]
    K --> L["(This is the file sent to the  
end user.)"]
  
```

FIG 13

```

graph TD
    82[(database.dat)] --> 86[Read footer tag  
(Including Database Key)]
    86 --> 88[Using the Database Key from the footer tag,  
unkey byte 1 in file.]
    88 --> 90[Update the key for the next byte]
    90 --> 92[Calculate a running checksum]
    92 --> 94[Repeat for each byte in master file]
    94 --> 96{Does calculated checksum match original  
file's checksum in the footer tag?}
    96 -- No --> 98[Stop and issue error message]
    96 -- Yes --> 98a[Wait for GPS unit to send identification  
packet containing GPS unit type and Database Key.]
    98a --> 100{Does the unit type match the database  
type of file?}
    100 -- No --> 102[Stop and issue error message]
    100 -- Yes --> 104{Does the Database Key received match the  
Database Key in file?}
    104 -- No --> 106[Stop and issue error message]
    104 -- Yes --> 108[Using Database Key sent from the GPS unit,  
unkey byte 1 in file.]
    108 --> 110[Update the key for the next byte]
    110 --> 112[Repeat until packet size is full.]
    112 --> 114[Send packet of unkeyed data to the GPS unit.]
    114 --> 116[Repeat until all bytes for database.dat file  
are processed.]
    116 --> 118([GPS Unit])
    118 --> 108

```

FIG 14

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

COPY PROTECTION FOR DATABASE UPDATES  
TRANSMITTED VIA THE INTERNET

the specification of which (check one)

- (x) is attached hereto.  
( ) was filed by an authorized person on my behalf on \_\_\_\_\_ as Application Serial No. \_\_\_\_\_ and was amended on \_\_\_\_\_.  
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and so identified, and I have also identified below any foreign application for patent or inventor's certificate on this invention filed by me or my legal representatives or assigns and having a filing date before that of the application on which priority is claimed.

| <u>Number</u> | <u>Country</u> | <u>Day/Month/Year Filed</u> | <u>Priority Claimed (Yes or No)</u> |
|---------------|----------------|-----------------------------|-------------------------------------|
|---------------|----------------|-----------------------------|-------------------------------------|

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

| <u>Application Serial No.</u> | <u>Filing Date</u> | <u>Status</u> |
|-------------------------------|--------------------|---------------|
| 60/021,702                    | July 12, 1996      | Pending       |



I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith and request that all correspondence in respect to this application be directed to FITCH, EVEN, TABIN & FLANNERY, Suite 900, 135 South LaSalle Street, Chicago, Illinois 60603-4277, Telephone No. (312) 372-7842:

| <u>Attorney</u>      | <u>Reg. No.</u> | <u>Attorney</u>    | <u>Reg. No.</u> |
|----------------------|-----------------|--------------------|-----------------|
| Morgan L. Fitch, Jr. | 17,023          | Robert J. Fox      | 27,635          |
| Francis A. Even      | 16,880          | Kenneth H. Samples | 25,747          |
| Julius Tabin         | 16,754          | Philip T. Petti    | 31,651          |
| John F. Flannery     | 19,759          | John S. Paniaguas  | 31,051          |
| Robert B. Jones      | 20,135          | Donald A. Peterson | 18,647          |
| James J. Schumann    | 20,856          | John J. Cavanaugh  | 18,372          |
| R. Steven Pinkstaff  | 20,448          | James R. McBride   | 24,275          |
| James J. Hamill      | 19,958          | James A. Sprowl    | 25,061          |
| Timothy E. Levstik   | 30,192          | Bruce R. Mansfield | 29,086          |
| Joseph E. Shipley    | 31,137          | Richard P. Beem    | 32,961          |
| Bryant R. Gold       | 29,715          | Richard A. Kaba    | 30,562          |
|                      |                 | Karl R. Fink       | 34,161          |

Full name of sole or one joint inventor:

KELLY EUGENE DILLARD

Inventor's signature:

*Kelly Eugene Dillard*

Date:

5/21/97

Residence:

OLATHE, KANSAS 66061  
(City and State for U.S. Residents;  
City and Country for others);

Post Office Address:

1817 FERREL DR.

OLATHE, KANSAS 66061

Citizenship:

UNITED STATES OF AMERICA

Full name of sole or one joint inventor:

DAVID LAWRENCE GODDARD

Inventor's signature:

*David Lawrence Goddard*

60323/462-96-004

Date: 5-21-97

Residence: KANSAS CITY, KANSAS 66106  
(City and State for U.S. Residents;  
City and Country for others);

Post Office Address: 6339 BERRY RD.  
KANSAS CITY, KANSAS 66106

Citizenship: UNITED STATES OF AMERICA

Full name of sole or one  
joint inventor:

DAVID LYNN SMITH

Inventor's signature:

David Lynn Smith

Date:

May 15, 1997

Residence:

OLATHE, KANSAS 66062  
(City and State for U.S. Residents;  
City and Country for others);

Post Office Address:

553 N. MUR-LEN, #300

OLATHE, KANSAS 66062

Citizenship:

UNITED STATES OF AMERICA

Address for Correspondence: FITCH, EVEN, TABIN & FLANNERY  
135 South LaSalle Street-Suite 900  
Chicago, Illinois 60603-4277

Declaration 0194-2

20250601 000000